



Calhoun: The NPS Institutional Archive DSpace Repository

Theses and Dissertations

1. Thesis and Dissertation Collection, all items

2014-12

Designing incentives for Marine Corps cyber workforce retention

Hernandez, Lucas F.; Johnson, Derek K.

Monterey, California: Naval Postgraduate School

<http://hdl.handle.net/10945/44578>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



<http://www.nps.edu/library>

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community.

Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

DESIGNING INCENTIVES FOR MARINE CORPS CYBER WORKFORCE RETENTION

By: **Lucas F. Hernandez, and**
Derek K. Johnson
December 2014

Advisors: **Thomas L. Albright, and**
Anita M. Salem

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE
Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE December 2014	3. REPORT TYPE AND DATES COVERED MBA Professional Report	
4. TITLE AND SUBTITLE DESIGNING INCENTIVES FOR MARINE CORPS CYBER WORKFORCE RETENTION		5. FUNDING NUMBERS	
6. AUTHOR(S) Lucas F. Hernandez and Derek K. Johnson			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) United States Marine Corps Programs & Resources Department (P&R) William McNavage (william.menavage@usmc.mil)		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number <u>N/A</u> .			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE		
13. ABSTRACT (maximum 200 words) There is a pervasive national shortage of qualified cyber personnel, both in the Marine Corps and the nation at large. To retain quality cyber personnel, the Marine Corps must identify those factors that cause cyber personnel to separate from active service and explore specific incentives to retain them. This research used Grounded Theory and Design Thinking to explore these challenges. Key findings show the importance of tailoring retention policies across three areas: monetary rewards (money and benefits), non-monetary rewards (duty station preference, geographic stability, educational opportunities), personal needs (development of transferrable skills and external career opportunities, internal career progression, alignment with personal interests and goals, access to technology), and organizational elements (allowance for community uniqueness, engagement of stakeholders in process development, and a healthy command climate with limited bureaucracy). These findings were incorporated into a Design Thinking process that resulted in three prototype solutions to cyber retention. This study demonstrates how the unique characteristics of cyber personnel require tailored incentive packages and improved personnel policies in order to foster employees' intrinsic motivations to achieve success. The results focus on the Marine Corps, but the underlying motivations should resonate with cyber personnel in any organization.			
14. SUBJECT TERMS Marine Corps, retention, cyber personnel, non-monetary incentives, intrinsic motivation, Design Thinking, Grounded Theory		15. NUMBER OF PAGES 81	
16. PRICE CODE			
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**DESIGNING INCENTIVES FOR MARINE CORPS CYBER WORKFORCE
RETENTION**

Lucas F. Hernandez, Captain, United States Marine Corps
Derek K. Johnson, Captain, United States Marine Corps

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

**NAVAL POSTGRADUATE SCHOOL
December 2014**

Authors: Lucas F. Hernandez

Derek K. Johnson

Approved by: Dr. Thomas L. Albright, Professor

Anita M. Salem, Research Associate

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

DESIGNING INCENTIVES FOR MARINE CORPS CYBER WORKFORCE RETENTION

ABSTRACT

There is a pervasive national shortage of qualified cyber personnel, both in the Marine Corps and the nation at large. To retain quality cyber personnel, the Marine Corps must identify those factors that cause cyber personnel to separate from active service and explore specific incentives to retain them. This research used Grounded Theory and Design Thinking to explore these challenges. Key findings show the importance of tailoring retention policies across three areas: monetary rewards (money and benefits), non-monetary rewards (duty station preference, geographic stability, educational opportunities), personal needs (development of transferrable skills and external career opportunities, internal career progression, alignment with personal interests and goals, access to technology), and organizational elements (allowance for community uniqueness, engagement of stakeholders in process development, and a healthy command climate with limited bureaucracy). These findings were incorporated into a Design Thinking process that resulted in three prototype solutions to cyber retention. This study demonstrates how the unique characteristics of cyber personnel require tailored incentive packages and improved personnel policies in order to foster employees' intrinsic motivations to achieve success. The results focus on the Marine Corps, but the underlying motivations should resonate with cyber personnel in any organization.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	THE IMPORTANCE OF CYBER SECURITY	1
B.	THE PROBLEM OF RETAINING CYBER PROFESSIONALS.....	2
C.	THE ROLE OF INCENTIVES IN RETENTION.....	2
D.	PURPOSE OF THE STUDY	4
E.	NATURE OF THE STUDY	5
F.	RESEARCH QUESTIONS.....	6
G.	SCOPE, ASSUMPTIONS, AND LIMITATIONS	6
II.	BACKGROUND	7
A.	THE DOD APPROACH TO RETENTION.....	7
B.	RETENTION MOTIVATIONS	8
1.	The Need for a Tailored Approach	14
C.	CURRENT RETENTION INCENTIVES FOR USMC CYBER WORKFORCE	16
D.	CYBER WORKFORCE CHARACTERISTICS	17
1.	Cyber Workforce Personality.....	18
2.	Cyber Motivations and Retention Strategies	18
E.	CYBER WORKFORCE RETENTION CHALLENGES.....	19
III.	METHODOLOGY	23
A.	COLLECTING CYBER STAKEHOLDER INFORMATION.....	24
1.	Population.....	25
2.	Primary Discussion Points	25
B.	THE DESIGN THINKING WORKSHOP.....	27
1.	About Design Thinking	27
2.	Principles of Design Thinking.....	27
3.	Design Thinking Process	28
IV.	RESEARCH FINDINGS.....	31
A.	INCENTIVES.....	32
1.	Monetary Incentives	32
a.	<i>Monetary Incentives Are Not Sufficient</i>	33
2.	Non-monetary Incentives	34
3.	Duty Station Preference and Geographic Stability.....	34
a.	<i>Duty Station Preference Matters</i>	35
b.	<i>Geographic Stability is Important</i>	35
4.	Education.....	36
5.	Transferrable Skills, Experience, and External Career Opportunities.....	36
6.	Internal Career Progression	37
a.	<i>Career Opportunities are Desired</i>	37
b.	<i>Career Roadmaps are Needed</i>	38

c.	<i>Barriers to Promotion Reduce Retention</i>	38
d.	<i>Absence of Middle Management Limits Growth</i>	39
B.	INTRINSIC MOTIVATORS	39
1.	Personal Factors	39
a.	<i>Personal Interests and Goals Influence Retention</i>	39
2.	Cyber Culture and Relationships	41
C.	ORGANIZATIONAL INFLUENCES	42
1.	Access to Technology	42
2.	Process Development	43
3.	Command Climate and Bureaucracy	44
D.	PROTOTYPE SOLUTIONS	45
1.	Career Progression Prototype—Experts are Developed	45
2.	Closed prototype – Everyone is a Cyber Warrior	46
3.	Fluid Career Prototype—Pathways In and Out	46
V.	CONCLUSION AND RECOMMENDATIONS	49
A.	KEY STAKEHOLDERS AND THEIR INVOLVEMENT	50
1.	Individual Cyber Marines	50
2.	MARFORCYBER	51
3.	The Marine Corps	51
B.	RECOMMENDATION	51
C.	RECOMMENDATIONS FOR FURTHER RESEARCH	52
D.	FINAL WORDS	53
APPENDIX. COLLABORATION QUESTIONS		55
DISCUSSION POINTS		55
FOLLOW UP QUESTIONS		55
LIST OF REFERENCES		57
INITIAL DISTRIBUTION LIST		63

LIST OF FIGURES

Figure 1.	Fiscal Year 2010 Major Components of Military Compensation for Active Duty Personnel (from the Eleventh Quadrennial Review on Military Compensation 2012)	14
-----------	---	----

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	The Paradigm Shift in Management (from Thomas and Jansen, 1996)	4
Table 2.	FY15 Selective Reenlistment Bonus for USMC MOS 0689, Cyber Security Technician	17

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACIP	Aviation Continuation Incentive Pay
ACOL	annualized cost of leaving
ACP	Aviation Continuation Pay
CRAM	Combinatorial Retention Auction Mechanism
CSRB	Critical Skills Retention Bonus
DCWS	Department of Defense Cyberspace Workforce Strategy
DOD	Department of Defense
DON	Department of the Navy
ELINT	Electronic Intelligence
GAO	United States Government Accountability Office
IT	Information technology
MARADMIN	Marine Administrative Message
MARFORCYBER	Marine Corps Forces Cyberspace Command
MOS	military occupational specialty
NPS	Naval Postgraduate School
NMI	non-monetary incentive
SRB	Selective Reenlistment Bonus
STEM	science, technology, engineering, and mathematics
SWO	Surface Warfare Officer
UIP	Universal Incentive Package
USCYBERCOM	United States Cyber Command
USMC	United States Marine Corps

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank the Marines of Marine Corps Forces Cyberspace Command for assisting our efforts and affording us the opportunity to conduct the collaborations. This project would not have been possible without your input. We hope this project will benefit you and your families at some point in your careers.

To the men and women who participated in the design process, thank you for sacrificing your e-week. Your experience and insight were invaluable.

Thank you to our advisors, Dr. Tom Albright and Anita Salem. Your patience and guidance were greatly appreciated. Thank you for opening our minds to this process and for having the trust and confidence that allowed us to explore and develop our own ideas.

Finally, we wholeheartedly thank our wives, Arianna and Becky. Your patience, support, and “encouragement” carried us through. We could not have done it without you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE IMPORTANCE OF CYBER SECURITY

Since the 1970s, awareness of cyber security's role in national security has steadily increased. This increase in awareness was the result of increasing security breaches, hacking and other cybercrimes during the past four decades. Early federal efforts to combat cyber crime were reactive rather than proactive and were slowly implemented. Hacking telephone networks started in the 1970s, but the first anti-hacking law was not implemented until 1984. Previous attempts to implement such laws were not initially passed in Congress. Significant efforts to combat cyber crime did not happen until the 2000s when the Bush administration first implemented a series of measures to increase national efforts to combat cyber threats. In 2001, President Bush established the President's Critical Infrastructure Protection Board to work with industry experts to improve the Nation's cyber security situation and to develop a framework for a national cyber security strategy that was released in 2002 (Washington Post 2003). In 2013, President Obama stated the importance of cyberspace in our national security:

America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas." (Obama 2013)

The president made this statement prior to Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (whitehouse.gov 2013). This order was designed to kick start an improvement process for the Nation's cyber capabilities. As our adversaries continue to press attacks in cyberspace, the need for qualified cyber personnel to defend our networks and our national interests is clear—our national interests lie in the recruitment, training, and retention of highly trained cyber security specialists (Chief Information Officer 2013).

B. THE PROBLEM OF RETAINING CYBER PROFESSIONALS

Shrinking labor pools, competition with industry, and reduced military budgets are all impacting the ability to retain cyber professionals. In March 2013, General Alexander, then Commander U.S. Cyber Command (USCYBERCOM), stated, “The biggest challenge we currently face is generating the people we need to do this mission.” For the Marine Corps, the challenge is especially severe. By 2016, Marine Corps Forces Cyberspace Command (MARFORCYBER) will need to increase its cyber workforce by 800 Marines and civilians (Sanborn 2014). This is a four-fold increase from the current level of 200 Marines in less than two years. The problem is that there is not a large enough labor pool to support the growing national need for cyber personnel (Paul, Porche, and Axelband 2014). This problem is compounded by the loss of highly skilled military cyber professionals through attrition. In addition, industry competition for cyber personnel is increasing. According to the Bureau of Labor Statistics (2014), the private sector cyber security workforce is growing at three times the national average and the sector offers higher pay. The median pay for cyber professionals in the private sector is \$41.43 per hour or \$86,170 annually compared to \$32,814 annually for an active duty E-5 with six years of time in service (Defense Finance and Accounting Service 2013).

Despite the cyber workforce being a priority, reduced budgets and fiscal austerity in the DOD increases the difficulty of using monetary incentives for retention (DOD 2014). A small labor pool and industry competitions drive the need for a strong retention strategy that includes a compelling set of incentives that will resonate specifically with the cyber workforce.

C. THE ROLE OF INCENTIVES IN RETENTION

Incentives, defined broadly as a thing that motivates or encourages one to do something, should achieve maximum value for both the organization and the individual. For the organization, incentives are intended to improve the hiring, retention, and performance of cyber personnel. Retention is problematic for the Marine Corps since a significant amount of personnel leave its ranks annually (Anderson 2013). The

Department of Defense (DOD) Cyberspace Workforce Strategy (DCWS 2013) addresses this challenge by outlining six areas for improving our military's cyber strategy:

- **Establish a cohesive set of DOD-wide cyberspace workforce management issuances**
- **Employ a multi-dimensional approach to recruiting**
- **Institutionalize continuous learning with greater focus on evaluating the maturity of skills**
- **Retain qualified personnel**
- **Expand threat knowledge**
- **Understand crisis and surge requirements and options**

DCWS Focus Area 4 calls for improving retention through incentive programs that include both monetary and non-monetary incentives. Monetary incentives are typically manifested as bonuses in the DOD. Non-monetary incentives are non-financial in nature and can manifest in many different ways including education, health care, or time off. To meet the DCWS strategic retention goals, the USMC must bolster its incentive programs and administrative policies to adapt to the unique needs of cyber personnel. To do this, the Marine Corps must first develop an understanding of *why* its cyber personnel choose to depart service. If the Marine Corps uncovers the motivating or satisfying factors behind cyber personnel retention, it then can tailor its incentive packages to the needs of the personnel it seeks to retain. Further, investigating the dissatisfaction factors can prompt policy changes to reduce or eliminate those factors and their potential negative impact on retention (Ramlall 2004).

Incentives are closely tied to the concepts of extrinsic and intrinsic rewards. Extrinsic rewards are tangible or physical rewards given for accomplishing something. Intrinsic rewards are intangible rewards that satisfy human needs such as self-esteem and achievement. For inclusion in the Eighth Quadrennial Review, Thomas and Jansen (1996) wrote about the idea of intrinsic value, or the psychological rewards or benefits one receives from a set of tasks or missions, in terms of military compensation. Their discussion contrasted the current form of military management—Command and

Control—with a newer form of management—Collegial—that was emerging in the private sector (Table 1).

Table 1. The Paradigm Shift in Management (from Thomas and Jansen, 1996)

	OLD MANAGEMENT STYLE	NEW MANAGEMENT STYLE
MANAGER'S ROLE	Directing and controlling	Leadership and coaching
WORKER'S ROLE	Compliance	Self-management
WORKER'S MOTIVATION	Mostly extrinsic <ul style="list-style-type: none"> • No commitment to task • Responds to carrots and stocks controlled by management 	Mostly intrinsic <ul style="list-style-type: none"> • Committed to task • Gets rewards directly from doing the task well

Thomas and Jansen (1996) suggested that intrinsic rewards should be developed as a form of compensation to complement the current incentive packages and the emerging collegial management style inside the DOD. Pink's research (2009) suggested that extrinsic or tangible rewards can have a negative impact on intrinsic motivations, and they may undermine the underlying intrinsic reasons for doing particular work. Instead, intangible rewards such as autonomy, encouragement to work on additional projects, quick feedback, challenges, and clear cut goals are all means to give drive, or intrinsic motivation, to an individual (Pink 2009).

D. PURPOSE OF THE STUDY

The purpose of this study is to identify and analyze critical factors that cause USMC cyber workforce personnel to separate from active service and to offer recommendations for improving retention. This study also addresses how the Marine Corps can better implement the retention strategy as described in the DCWS. The data for this study was collected through a literature review, face-to-face collaborations with cyber stakeholders, and a design workshop that used a human-centered approach to problem-solving to address the strategic challenges in retaining military cyber personnel.

This study will present the results of our work and make recommendations to improve the retention of cyber personnel. These recommendations include:

- **Re-thinking how monetary incentives are utilized**
- **Designing new non-monetary incentives**
- **Improving policies**
- **Streamlining processes**
- **Fostering intrinsic motivations**

E. NATURE OF THE STUDY

The focus of this research was to develop an understanding of the type of personnel that comprise the cyber workforce and to explore their reasons for leaving military service. The study of previous works on retention, monetary and non-monetary incentives, and the significance of intrinsic motivation on the cyber warrior guided this research and our recommendations.

Research was conducted using grounded theory (Glaser and Strauss 1967). Charmaz (2006) describes grounded theory as a set of methods that “consist of systematic, yet flexible guidelines for collecting and analyzing qualitative data to construct theories ‘grounded’ in the data themselves.” Since quantifiable data in this case does not properly frame or address the underlying intrinsic motivation issues the Marine Corps faces with cyber personnel, this study focused on collecting qualitative data. Qualitative data was collected from face-to-face collaborations with cyber stakeholders and through a cyber-focused Design Thinking workshop conducted at The Naval Postgraduate School (NPS).

The face-to-face collaborations utilized a set of general questions that addressed policies, processes, culture, technology, and the physical environment within the Marine Corps’ cyber workforce and their impacts on retention. These questions were used as a stepping-stone into more specific questions to penetrate the core issue of retention. No two collaborations were the same. Each participant had a slightly different perspective. A strong set of patterns, however, emerged early on in the research.

F. RESEARCH QUESTIONS

Our collaborations with Marine Corps' cyber personnel and subsequent data analysis focused on answering two core research questions:

- **What are the critical retention issues that face the Marine Corps' cyber workforce and what are the factors that cause Marine Corps' cyber personnel to depart military service?**
- **What incentives, specifically non-monetary, would influence the retention of cyber personnel?**

G. SCOPE, ASSUMPTIONS, AND LIMITATIONS

This study addresses the retention issues that specifically affect the Marine Corps' cyber workforce. This study assumed that there is in fact a retention problem within Marine Corps' Cyber. This study did not address the issue of whether or not the cyber workforce was leaving the military at a higher rate than other military specialties. The results of collaborations between MARFORCYBER and the authors produced enough data to narrow the scope to address the Marine Corps and their specific retention issues. The findings contained in this paper may, however, prove useful across the DOD cyber workforce to help identify underlying retention issues.

II. BACKGROUND

A comprehensive literature review was conducted to gain foundational knowledge required to identify and examine critical factors that present retention challenges to the Marine Corps' cyber workforce. While this study's focus is on a distinct population within the U.S. military, the body of literature required to achieve an ample understanding of military cyber and retention strategies, incentives, and the cyber workforce necessitated an analysis of government and commercial industry publications, as well as previous scholarly reports. This chapter discusses the background research used to understand the forces effecting retention and incentives, their impacts on the cyber workforce, and the challenges faced in the DOD and USMC.

A. THE DOD APPROACH TO RETENTION

Each branch of service meets its individual end strength goals through various means. Among the various means are recruiting, monetary incentives, and non-monetary incentives. Overall, the DOD relies heavily on monetary incentives. Critical Skills Retention Bonuses (CSRB) is authorized for certain skills sets that are deemed "critical" such as Special Forces. Other specialties that have high private sector demand or high private sector pay are given bonuses or incentive pay to make up the disparity. For instance, Aviation Career Incentive Pay (ACIP) is used for aviators. Qualified personnel matter in highly technical fields such as aviation and cyber security (DOD 2014).

When bonuses or other types of monetary incentives are not enough, then other avenues are used. Civilians and sometimes private sector contractors are frequently utilized to fill the roles where the military has personnel shortfalls. U.S. Cyber Command (USCYBERCOM) was recently given congressional authority to direct hire civilian workers to make up for the lack of qualified cyber workforce personnel. Along with the authority to direct hire came incentives to help recruit civilians. USCYBERCOM was given authority to pay for moving expenses and to pay back student loans of newly recruited civilians. In addition, there is a special pay scale for civilians with highly sought after skills that can boost a civilians pay by over 40 percent. The problem with this tactic

is the danger of creating a revolving door. Highly qualified military personnel can leave the service and then get hired as civilians, doing the same jobs for more money (Libicki, Senty, and Pollak 2014). The DOD is given end strength authorization by Congress annually through a Defense Authorization Act. Each branch then makes annual adjustments to meet the requirements of that year's authorization act. As a result, retention is strictly a numbers game for the DOD. Each branch has x amount of jobs and y amount of people to fill those jobs. Kapp (2013) noted that the DOD Active Component retention performance goals were measured by a specific quantity of personnel based on career phase. The Reserves measure retention based on a ratio of personnel attrition rate that is not supposed to exceed a certain percentage. The Marine Corps, specifically, measures retention numerically based on first term or subsequent term(s) enlistments (Kapp 2013). Logically, as the number of jobs that need to be filled increases and the amount of people to fill those jobs decreases, the pool of available qualified personnel decreases. This shortage is especially painful in technical fields such as cyber security (DOD 2014).

B. RETENTION MOTIVATIONS

Recent studies of cyber professionals and their demographics do not find compensation as a primary motivator when seeking or remaining with a job (Conti and Raymond 2011; Semper Secure 2013). It is important to understand where motivations lie and what to consider when tailoring incentives for military personnel as a whole. Thomas and Jansen (1996) found that intrinsic motivation is an important factor to consider when addressing military attrition and retention. Contrasting intrinsic task motivation—that which involves psychological reward to the individual derived directly from a task—and extrinsic task rewards—task-contingent rewards given to an individual by others—, they discussed intrinsic task rewards as a major contributor to job satisfaction and an individual's subsequent decision to remain in the military (Thomas and Jansen 1996). Additionally, they concluded intrinsic task motivation and self-management (decision-making behaviors) of personnel are intimately related and have a positive impact on problem-solving skills: flexibility, adaptation, responsiveness, innovation, and learning (Thomas and Jansen 1996). All these factors are important to

leadership and the cyber workforce of today's military environment, and, ultimately, create positive effects on their retention.

There is an array of research on understanding the importance of intrinsic motivation and its impact on retention within the workplace. In 2005, Basset-Jones and Lloyd examined the relevance of Herzberg's (1959) two factor theory in the current work environment. Herzberg presented one of the first theories to argue that there was a weak correlation between financial reward and job satisfaction. Herzberg, as cited in Samuel and Chipunza (2009), argued that employees were motivated by internal values, which he called "motivators." These motivators were intrinsic variables: the work itself, responsibility, achievement, and growth. He argued external values such as salary, policy, and supervisor/co-worker relationships, which he called "hygiene factors," were extrinsic variables that, although necessary in the workplace, did not motivate employees (Samuel and Chipunza 2009). Further, Basset-Jones and Lloyd (2005) stated that Herzberg felt motivation was generated from internal desires and growth needs, rather than externally stimulated incentives. They asserted,

Motivation is founded upon satisfaction born of a sense of achievement, recognition for achievement, responsibility and personal growth. Herzberg went on to suggest that recognition for achievement translated into direct feedback; responsibility into self-regulation, authority to communicate, exercise of control over resources and accountability; whilst advancement and growth translated into the central dynamic of new learning leading to new expertise. (Basset-Jones and Lloyd 2005, 934)

The Basset-Jones and Lloyd (2005) research found motivators based on intrinsic drivers were more instrumental to employee contribution than incentives based on extrinsic rewards such as "financial inducements" or observing others benefit from recognition. They further criticized theories founded on extrinsic "incentivisation" based on money and gifts being instrumental to employee contribution as being largely erroneous (Basset-Jones and Lloyd 2005). They concluded a significantly greater amount of employees are influenced from a desire to overcome frustrations and contribute to the organizational success, rather than from financial inducements (Basset-Jones and Lloyd 2005). Basset-Jones and Lloyd (2005) also cautioned organizations to consider the extent to which they rely on extrinsic incentives to induce employee actions. They warned that

extrinsic motivators promoted a need for consistent additional rewards which may not be sustainable during financially unstable times when retaining talent and fostering new ideas may be needed most (Basset-Jones and Lloyd 2005).

In 2009, Samuel and Chipunza conducted further research on the impacts of intrinsic and extrinsic factors on the growing need to retain the best quality employees within organizations that were faced with external competition. Their study contrasted the theoretical background of Herzberg's (1959) two factor theory of intrinsic factors with several other empirical studies which identified extrinsic factors as key motivational variables that influenced retention. Samuel and Chipunza (2009) concluded that a combination of both intrinsic and extrinsic variables should be used by organizations for an effective retention strategy. Their study found that the following motivational variables had significantly influenced employee retention in both the public and private sectors: training and development, challenging/interesting work, freedom for innovative thinking, and job security (Samuel and Chipunza 2009). They further challenged their own findings by citing Bussin (2002) who argued that "constant training and development of employees' skills can indeed facilitate their early turnover instead of reinforcing their retention. Providing employees with the latest training and development opportunities raises their market value thus increasing their mobility" (Samuel and Chipunza 2009). Samuel and Chipunza (2009), however, ultimately concluded that training and development greatly appealed to employees and was one of the key factors in retaining them. They determined that training and development enhanced employee performance and encouraged retention, especially in an organization with a programmed training system that is tailored towards career progression (Samuel and Chipunza 2009). These findings should be closely examined and considered when accounting for the structured training environment within the military.

In 2009, Kenneth Thomas went a step further and developed a motivational model to adapt to the younger population of workers. These workers were described very similarly to the way many cyber professionals are described. According to Thomas (2009), these workers were "raised in an era of rapid technological change and instant

access to data, they respond best to work that is meaningful, allows them to learn cutting-edge skills, and lets them find their own ways of accomplishing tasks.”

Thomas (2009) found the nature of today’s workplace required a significant degree of self-management, and employees discovered value in innovating, problem-solving, and improvising to meet the conditions encountered. Contrasting the use of extrinsic and intrinsic rewards in the workplace, he asserted,

Extrinsic rewards remain significant for workers, of course. Pay is an important consideration for most workers in accepting a job, and unfair pay can be a strong de-motivator. However, after people have taken a job and issues of unfairness have been settled, we find that extrinsic rewards are now less important, as day-to-day motivation is more strongly driven by intrinsic rewards. (Thomas 2009)

Thomas’ (2009) model described four important intrinsic rewards for workers that potentially created a positive emotional charge and reinforced active self-management and engagement in their work. These were:

- **Sense of meaningfulness.** This reward involved a strong sense of purpose or direction. Workers felt they have the opportunity to accomplish something of real value that is worth their time and efforts.
- **Sense of choice.** Workers felt they have the ability to use their best judgment to choose how to accomplish their work. This gave them ownership and responsibility for the paths they took.
- **Sense of competence.** Workers felt their performance of work activities was up to standards and of high-quality. They felt a sense of satisfaction and pride in how well they performed their duties.
- **Sense of progress.** Workers felt encouragement that their efforts actually accomplished something and headed in the right direction. This gave them confidence in their choices and future. (Thomas 2009)

Thomas’ (2009) research found widespread benefits from these intrinsic rewards for both organizations and employees. For organizations, intrinsic rewards were strong predictors for the “right” kind of retention. Intrinsic rewards kept those “who are energized and self-managing rather than those who can’t afford to leave” (Thomas 2009). The intrinsic rewards also led to positivity in workers’ recommendations, which served as recruiting and marketing tools for organizations (Thomas 2009). For employees, the

intrinsic rewards provided a healthy and sustainable source of motivation, resulting in increased job satisfaction, professional development, and lower stress (Thomas 2009). According to Thomas (2009), intrinsic rewards created a strong “win/win” for both the organization and its employees. The performance-driven aspect of intrinsic rewards is attractive to today’s workplace, and the rewards are feasible during fiscally constrained times because they do not require large outlays of money to generate extra effort (Thomas 2009). These factors are particularly appealing to the DOD given the current defense environment.

Upon analyzing why service members choose to depart military service, research shows they leave based on an internal cost-benefit analysis which determines that the benefits of leaving are greater than the benefits for staying. This is otherwise known as the Annualized Cost of Leaving (ACOL) approach (Riebel 1996). Further, financial benefits do not affect long-term solutions to the retention problem. For instance, Riebel (1996) conducted a study that analyzed the retention effects of aviation incentive pay on naval aviators using an ACOL approach. ACOL was developed in 1984 by Warner and Goldberg to try to predict whether a service member would depart from active service or not. The study describes the service member’s thought processes and ultimately determined that the individual would do a cost-benefit analysis to determine the benefits and costs of leaving or staying in the service. The cost of leaving may not be strictly financial, but also may be in terms of personal values that matter to the individual. For cyber personnel, this may relate to why bonuses are not necessarily an effective means of retention (Semper Secure 2013). Typically, the military uses bonuses to increase the cost of leaving to prevent service members from departing service. For example, the Aviation Continuation Pay (ACP) bonus targets certain aviators deemed valuable in exchange for extending their service commitment. Riebel found that ACP was more cost effective because it can be used to target a specific community of aviators, unlike Aviation Continuation Incentive Pay (ACIP), which is an entitlement that all aviators receive from the start of their flying career. Increasing ACIP was cost effective in retaining aviators but not as much as ACP. Riebel’s study used the cost of training aviators and not the cost of replacement. The cost of replacement is higher (than the cost to train) and the net

benefit for increasing ACP would also be higher. The use of targeted bonuses, like ACP, instead of incentive pay for the cyber workforce may be seen as more effective because of similarities drawn between the technical nature of aviation and cyber fields. If aviators and cyber personnel are similar, then this validates the DOD's use of bonuses for cyber personnel. Targeted bonuses then increase the cost of leaving active service and, as a result, the targeted person is more likely to stay.

In technical fields, such as cyber, intrinsic factors may have a stronger long-term positive impact on the retention problem. The intangible forces that affect individual motivation result in higher morale, higher productivity, and decreased burn-out rates (Pink 2009). Congressman Skelton (1999) for instance, suggested that *esprit* made a difference when unit deployments were at a high and the force was shrinking. In other words, unit morale was high at a time when morale seemingly should be low. Congressman Skelton (1999) continues further by combining *esprit*, morale, and cohesion as key factors for retention. These intrinsic factors cannot be affected by Congress or senior leadership, but only by "deckplate" leadership (Skelton 1999). Congressmen Skelton's ideas relate to Thomas and Jansen's (1996) work on intrinsic compensation. *Esprit* can be seen as a form of intrinsic compensation that monetary compensation competes with.

Pink (2009) made observations similar to Congressman Skelton. Pink agreed that intrinsic motivations are crucial for creating an environment of success and productivity where people want to work. Creating a system that leaves out the fundamental intrinsic motivations behind an individual's work will fail in the long run. A system that uses contingent rewards—often cash incentives offered to achieve a certain objective—are good for short-term motivation. An example of a contingent reward is a bonus for signing a four-year reenlistment. In the long-term, the person being offered the reward is stripped of drive. According to Pink (2009), drive is stripped away because once pay is used as a motivator then the intrinsic motivation of that person is gone and job satisfaction decreases. The highest job satisfaction is achieved outside of extrinsic motivators. Strong intrinsic motivators include: autonomy, mastery, and purpose. The perception of autonomy increases performance and morale. Mastery and purpose are also closely

related. Mastery is the desire to constantly improve at a task, skill, or anything of the like because of a strong sense of purpose with clear and understood goals. Purpose is the push behind mastery. The push is the sense of a greater value behind what the person is trying to achieve (Pink 2009).

1. The Need for a Tailored Approach

Once a thorough understanding of intrinsic and extrinsic motivations is achieved, we can then examine the benefits of non-monetary incentives on military personnel. According to the Eleventh Quadrennial Review on Military Compensation (2012), noncash (“in-kind”) and deferred compensation (retirement and veterans benefits) account for nearly 50 percent of military compensation. Non-monetary incentives include health care, educational benefits, and on-base housing among other installation services and facilities (Figure 1).

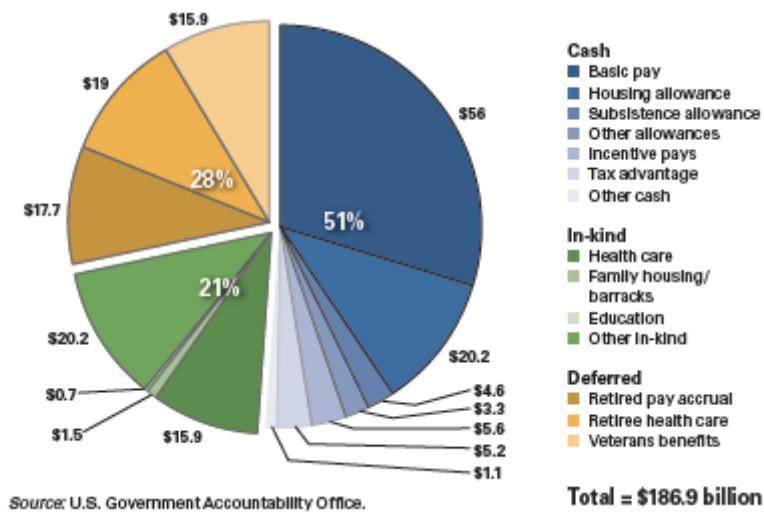


Figure 1. Fiscal Year 2010 Major Components of Military Compensation for Active Duty Personnel (from the Eleventh Quadrennial Review on Military Compensation 2012)

Coughlin, Gates, and Myung (2013) examined the one-size-fits-all approach to these current non-monetary incentives, and they concluded that the DOD could reduce the cost of military compensation by personalizing service members’ non-monetary incentive packages to reflect their individual needs and preferences. Three sources of

variation in preferences for non-monetary incentives were identified: variability across population classes (e.g., services, professional communities, rank/pay grade, etc.); variability across individuals within a population (e.g., the value of child care to service members with young children versus single service members); and variability across non-monetary incentive packages for an individual (e.g., service member may place a high value on one incentive over another but have minimal extra value for both over each individual one) (Coughlin, Gates, and Myung 2013). They discovered,

In fact, surveys across different military communities, ranks, and years of service, show the difficulty of identifying any NMI (non-monetary incentive) that has significant value for even 50 percent of the active duty force. At the same time, approximately 80 percent of the surveyed service members expressed a significant positive value for at least one NMI. (Coughlin, Gates, and Myung 2013, 27)

Coughlin, Gates, and Myung (2013) established that service members receive a diminishing marginal satisfaction from income, and as monetary incentives diminish in value, non-monetary incentives become more important. Further, providing a non-monetary incentive universally to all service members could cost the DOD much more than it creates value for the individual. Where service members' value exceeds the DOD's cost of provision, the DOD could reduce its costs by personalizing non-monetary incentives, thereby benefiting both parties (Coughlin, Gates, and Myung 2013).

Additionally, rather than using the current Universal Incentive Package (UIP), Browning and Burr (2009) experimented with the Combinatorial Retention Auction Mechanism (CRAM) that not only creates additional value to the service member but to the Navy as well. CRAM facilitates retention of personnel, for a single employer, by asking employees to place a reservation value on monetary and NMIs that they require to stay with the organization. The employer then selects the lowest costing employees to retain based on a predetermined number (Coughlan, Gates, and Myung 2013). The benefit to the Marine Corps is that a cyber security Marine could create his or her own incentive package thereby reducing the overall cost to the government and creating additional value to the Marine. Both stakeholders are better off in this case (Browning and Burr 2009).

Each community within the military has different values and responds differently to incentives. For instance, Browning and Burr (2009) concluded that the Navy Surface Warfare Officer (SWO) community, comprised solely of commissioned officers, was not sensitive enough to monetary incentives and explored NMIs that created value specifically to SWOs. Some examples of NMIs that SWOs valued, as investigated through a survey, are homeport choice, geographical stability, and sabbatical. Asch, et al (2010) suggests that Zone B reenlistees (Table 2) are also less affected by financial incentives. This loss of effect is a result of the service member's taste for service or changing desire to serve at various career decision points, such as reenlistment (Asch et al, 2010).

Harrison (2012) completed a study that analyzed data by rank, age, and years of service to determine how service members value different forms of compensation. Regardless of rank, service members highly value basic pay, and the most junior personnel place the highest value on basic pay. This benefit, however, is offset by the cost. Service members in the 18–29 age group placed the highest value on performance-based bonuses, but they valued it at only a fraction of what it would cost to implement the program (Harrison 2012). Harrison (2012) also found that a dollar increase in basic pay for the most junior enlisted has more than six times the effect than that same dollar increase has to a senior officer's pay.

C. CURRENT RETENTION INCENTIVES FOR USMC CYBER WORKFORCE

The DOD currently has an established retention incentive strategy directed towards its cyber workforce. Significant limitations of these incentives, however, have been identified. The DOD's Cyber Operations Personnel Report (2011) listed two cash compensation retention bonuses, the Selective Reenlistment Bonus (SRB) and the CSRB, as the primary means to achieve retention requirements for cyber-related occupational specialties. The Marine Corps' most current retention bonus for cyber-related occupational specialties was outlined in the Fiscal Year 2015 (FY15) Selective Reenlistment Bonus Program (USMC 2014). Table 2 illustrates what a Cyber Security

Technician, Military Occupational Specialty (MOS) 0689, could expect to receive for a 48-month reenlistment based on the member's current years of active service.

Table 2. FY15 Selective Reenlistment Bonus for USMC MOS 0689, Cyber Security Technician

<u>Zone A (17 mos. to 6 yrs.)</u>	<u>Zone B (6–10 yrs.)</u>	<u>Zone C (10–14 yrs.)</u>
\$46,500–\$51,000	\$52,500–\$58,000	\$35,250–\$39,250

As evidence of the Marine Corps' high demand for cyber professionals, these bonus payments were the highest offered within all three target zones for FY15 in the Marine Corps.

In addition to retention bonuses, the U.S. Government Accountability Office (GAO) conducted a study in 2011, which found the DOD offered the broadest range of incentives to recruit and retain cyber security professionals (Wilshusen and Melvin 2011). These incentives included relocation incentives, scholarship programs, student employment programs, and student loan repayment, among others. GAO (Wilshusen and Melvin 2011), however, concluded no data existed and no metrics were in place to measure the effectiveness of these incentives in the eight federal agencies studied. It is important to note the GAO study did not differentiate incentives within the DOD that were designed specifically for service member retention versus the civilian DOD workforce. The DOD will continue to face challenges in achieving its cyber workforce retention goals without these key measurement criteria.

D. CYBER WORKFORCE CHARACTERISTICS

One of the most challenging aspects of retaining the cyber workforce has been the notable difference in characteristics, motivations, and values. These differences are likely to impact the effectiveness of retention incentives.

1. Cyber Workforce Personality

As Conti and Raymond (2011) noted, the ideal cyber warrior has high technical aptitude, is a creative problem-solver, and enjoys manipulating and pushing complex systems and technology in unintended ways. They are often independent and possibly introverted, and they have a strong desire to be around intellectual peers and leaders (Conti and Raymond 2011). Their education and professional experience levels may be higher than most of their rank counterparts as well. The rapid advancement of technology and tactics in the field necessitates an individual that is hungry for knowledge and eager to take on intellectually challenging tasks. These differences within the cyber workforce may require different incentive structures that focus more on their desire for knowledge and an “intellect-centric” culture (Conti and Raymond 2011). Incentives that incorporate access to new hardware/software, further training and certifications opportunities, and a flexible and dynamic work environment may be of more interest to cyber professionals than monetary bonuses.

2. Cyber Motivations and Retention Strategies

Recent surveys of cyber professionals have also found that compensation is typically not one of the most important factors when considering a job (Semper Secure 2013). These individuals have a sincere interest in their employer and the type of work they do. The Cyber Security Census conducted by Semper Secure (2013), and underwritten by Northrup Grumman among others, surveyed 500 cyber security professionals (14 percent of which were in the government sector and 13 percent in the Defense/Aerospace sector) and found the most important factor of a job is access to technology. In addition, control over work and its environment as well as work flexibility both ranked above compensation and benefits (Semper Secure 2013). In contrast, the same survey found that high total compensation was highly important to cyber security professionals when considering overall quality of life—second only to flexible work arrangements. The Cyber Security Census (2013) concluded that the top retention strategies for businesses were:

- **Professional Development:** Cyber security professional want to be challenged and to move up. Provide opportunities to develop your current employees so they do not become your future competition. (slide 21)
- **Support New Educational Programs:** Foster interest in the field early on through tailored educational work-study programs. (slide 21)

E. CYBER WORKFORCE RETENTION CHALLENGES

Military service and sacrifice go hand-in-hand. Service members give up freedoms and some normalcy that the private sector has. Unfortunately, the sacrifices weigh heavily on service members when they are deciding to stay or leave. Factors that influence leaving the military include: hours, schedules, deployments, moving every two to three years, and negative impact on family life. Linn (2009) conducted research surveys which showed that the main reasons people leave the Navy are basic pay, family and personal time, quality of leadership, and deployments. Self-reported weekly work hours for enlistees average 54 hours per week while officers average 60 hours per week (Linn 2009). The long work hours along with fluctuating schedules, deployments, and overnight duty take a toll on families by reducing personal time with them. Spouses that seek employment have a more difficult time keeping employment and are often paid less than their counterparts. Typically service members change duty stations every two to three years. These changes impact children's schooling and spouses' careers. If a spouse left a career to move with their spouse then that additional sacrifice weighs on the relationship.

Linn (2009) recommended several ways to improve retention for senior information warfare officers and found that both monetary and non-monetary incentives improve retention. Monetary incentives are seen as typically a short-term solution while non-monetary means are a long-term solution to retention. Non-monetary incentives, when properly designed, improve morale and intrinsic motivation. Improved training toward expertise, guaranteed geographic stability after department head tour, funded education, and sabbaticals are ways that surveys of the surface warfare officers found to improve retention of that community (Linn 2009).

While some recent signs indicate the DOD's cyber workforce retention problem may be overstated, the challenges to retain qualified cyber personnel are not temporary. U.S. Army Colonel Robert J. Turk (2013) noted that General Keith Alexander, then Commander of U.S. Cyber Command and Director of the National Security Agency, as well as Vice Admiral Michael Rogers, Commander of the Navy's Fleet Cyber Command, and Lieutenant General Michael Basia, the Air Force's Chief Information Officer, all testified before Congress in 2012 that their cyber workforces were opting to remain in service and not departing for industry as initially feared. When they do depart, it will most likely be for a combination of monetary and non-monetary reasons:

Nonetheless, while the DOD retention numbers have remained high, as the economy continues to rebound, so will the demand for cyber-security personnel in private industry. These factors contribute greatly to skilled personnel taking jobs and moving quickly for more pay, and/or responsibility. (Turk 2013, 15)

According to Turk (2013), cyber professionals have seen an 11 percent annual increase in compensation from 2010 to 2013. These figures have continued to rise as cyber security has played an important role in all sectors of industry. ClearanceJobs.com's 2013 Compensation Survey (Lesser 2013) results found while compensation for security-cleared military personnel fell 5.4 percent annually to \$64,601 from 2012 to 2013, the cyber security field reported average annual salaries alone of \$88,092 during the same period. ClearanceJobs.com's 2014 Compensation Survey (Lesser 2014) again reported a one percent increase on average in overall compensation for cyber security professionals. The survey also addressed the increased competition for cyber professionals within the government and private sectors:

The government and its contractors have a pressing need for tech talent, including most acutely cybersecurity professionals. The rub: so does every other industry. The national unemployment rate for technology professionals is 2.9 percent in February, as measured by the Bureau of Labor Statistics. (Lesser 2014, 5)

In the current austere fiscal environment of the federal government with additional planned drawdowns, the military finds itself in a difficult position to effectively compete with the private sector for retention of cyber professionals. While the

services are being forced to cut spending and become more efficient with dwindling resources, the private sector is thriving in a strengthening economy. In 2013, (ISC)², in partnership with Booze Allen Hamilton, conducted the Global Information Security Workforce Study (Suby 2013) which was designed to “gauge the opinions of information security professionals regarding trends and issues affecting their profession and careers.” They surveyed 12,396 respondents from numerous industries including government, defense, and private enterprise from around the world. The study reported qualified security staff is one of the most important key tools in information security, and 56 percent of respondents reported that their organizations possesses too few information security workers (Suby 2013). Further, the study found that an increase in spending for information security personnel and resources was predicted by one-third of the respondents; however, the government and defense sector were more prevalent in the 10 percent of respondents who predicted decreases in spending (Suby 2013). This data is important when predicting challenges the DOD could face in long-term retention of cyber professionals.

Kapp (2013) took a historical perspective on this matter and compared the DOD’s current retention challenges with those which occurred during the Post-Cold War force reductions. During the 1990s, all of the services initially reported excellent recruitment and retention after the initial drawdown due to reduced goals for each; however, by the late 1990s, most services began to experience recruitment and retention shortfalls (Kapp 2013). Some of the perceived causes included competition with a robust civilian economy, competition with institutions of higher education, and demographic and attitudinal changes among younger Americans (Kapp 2013). As current force reductions and budgetary constraints impact the military workforce, Kapp (2013) concluded that recruitment and retention will likely remain favorable in the short-term. Ultimately, if factors negatively impact job satisfaction, a perception of limited advancement prospects is created, or the economy continues to improve making the civilian sector more attractive, then recruitment and retention challenges may become more prevalent (Kapp 2013).

Ultimately, it is widely admitted that the DOD cannot compete with the private sector on compensation. The DOD Cyber Operations Personnel Report (2011) lists pay and incentives as the number one challenge for recruiting and retention of cyber personnel. Compounding the issue is the fact that only 25 percent of the typical recruiting pool of 18 to 24 year-olds is qualified for service (DOD 2011). Most individuals are automatically disqualified for a variety of factors including: education, quality of education, physical and mental fitness, and medical related issues (DOD 2011). Compensation continually arises as a major concern when trying to compete for the limited availability of qualified personnel in the cyber arena.

The literature review achieved a solid knowledge base for the conduct of this study. It shows that a unique approach is required to adequately address the retention challenges that face the cyber workforce. While monetary incentives are important, they may not achieve the intrinsic rewards that cyber personnel look to gain from their work. The Marine Corps must ensure they recognize and consider the particular needs of its cyber workforce when aligning its retention strategy with that of the DCWS.

III. METHODOLOGY

The purpose of this study was to identify and analyze critical factors that cause USMC cyber workforce personnel to separate from active service and to explore the design of non-monetary incentives that would influence their retention. This study used qualitative methods and grounded theory to explore the human factors impacting retention and then applied Design Thinking to look at possible solutions. The grounded theory methodology was chosen based on several key elements of qualitative research described by Snape and Spencer (2003): The study aimed to provide an in-depth understanding of the social world, circumstances, experiences, and perspectives of the research subjects; it utilized a small scale and a purposefully selected sample; it used data collection methods which involved close contact between research participants that were interactive and emergent (e.g., collaborations and discussions); and it utilized analysis that was open to emergent concepts and ideas to identify patterns or develop explanations. Additionally, Corbin and Strauss (1990) described grounded theory as an interactive approach to uncover both the relevant conditions at work and how the actors respond to changing conditions and the consequences of their actions. There were four major phases conducted for this study: background research, collaborations with stakeholders, exploration of designing incentives, and final analysis of findings.

The first phase of the study was the background research conducted through a comprehensive literature review to gain an ample understanding of the forces affecting retention, the nature of the cyber workforce, and their roles in the DOD and USMC. The literature review was used to identify significant existing concepts on the research topic and as a tool to formulate questions to act as a stepping off point for subsequent phases of the study (Strauss and Corbin 1998).

The second phase involved in-person collaborations with Marine Corps' cyber personnel, or stakeholders, to gather design ideas related to retention motivations. An informal in-depth interview design was chosen as an unstructured data collection tool due to the complex nature of the research problem and the varying personal contexts (Lewis 2003).

The third phase included presenting the findings of the literature review and informal discussions within a Design Thinking workshop to stimulate ideas for the design of retention strategies for Department of the Navy (DON) cyber personnel. This process was chosen for its innovative and human-centered approach to the complexity of the research problem (Brown 2009).

Lastly, the final phase analyzed all data from each previous phase and addressed findings that could potentially strengthen the Marine Corps' cyber retention strategy, as well as identify opportunities for follow on research. This analysis and presentation aimed to provide explanatory accounts which could lead to further consideration of policy realignment (Ritchie, Spencer, and O'Connor 2003).

As Chapter II already addressed the literature review in depth, this chapter provides the detailed methodology of phases two and three of this study. Chapter IV addresses the final phase of analysis.

A. COLLECTING CYBER STAKEHOLDER INFORMATION

A visit was conducted to Marine Corps Forces Cyberspace Command located in Fort Meade, Maryland, in order to accomplish in-person collaborations with personnel actively involved in cyber operations. These collaborations were essential in identifying relevant and important factors impacting retention as perceived by stakeholders within the Marine Corps' cyber workforce. Nine informal discussions were conducted using an in-depth interview design, which Legard, Keegan, and Ward (2003) described as "one of the main methods of data collection used in qualitative research."

To protect the individuals who participated in the collaborations, verbal informed consent was used to ensure participants understood both the nature of the collaboration and that they were participating voluntarily. Additionally, participants were verbally informed that their privacy and anonymity would be protected, and no personal identifiable information other than rank and MOS would be collected.

1. Population

The collaboration population consisted of nine participants of varying ranks and MOSSs consisting of:

Rank: (2) Captains; (1) Master Gunnery Sergeant; (2) Gunnery Sergeants;

(1) Staff Sergeant; (2) Sergeants; (1) Corporal

MOS: (5) 0689: Cyber Security Technician; (2) 2631: Electronic Intelligence (ELINT) Intercept Operator/Analyst; (1) 0605: Cyber Network Operations Officer; (1) Artillery Officer

The participant sample was small in size due to the qualitative nature of the study. According to Ritchie, Lewis and Elam (2003), qualitative research samples are usually small for three reasons: first, properly analyzed data will reach a point of diminishing return where increases in sample size will not provide new evidence; second, statements of incidence or prevalence are not the goal of the research; and third, heavily detailed information is gained from qualitative research which requires intensive resources. Patterns on perceived issues and ideas for improvement of retention within the Marine Corps' cyber workforce were recognized early in the collaborations even with a small sample size (Crouch and McKenzie 2006). Purposive sampling was conducted based on very specific criteria (i.e., MOS, duty location, etc.); therefore, the data collection method chosen and the small population and limited access of Marine cyber personnel imposed limitations on the sample population. These limitations also impacted the diversity of our population. While the diversity was not measured to the entirety of the Marine Corps' cyber professionals due to time and resource constraints, steps were taken to ensure a range of ranks and MOS were represented. Further, as this study was focused on the retention of active duty service members, no discussions with DOD civilian employees were conducted.

2. Primary Discussion Points

The questions asked during the collaborative process were designed to elicit ideas on retention incentives for use in the follow on phases of this study. The questions were

focused on the impact of multiple factors on retention of the Marine Corps' cyber workforce as a whole, rather than an individual's personal decision to remain on or depart active service. Questions were open-ended and strictly qualitative in nature (see Appendix). The following two primary discussion points were used to focus participants and stimulate ideas on the theme and context of the research (Legard, Keegan, and Ward 2003):

- **What things influence a cyber professional to join the Marine Corps?**
- **What things influence a cyber professional to stay in the Marine Corps?**

Based on a systems theory approach and organizational change models, follow up questions were designed to address the idea of a multiplicity of factors, their interrelationships, and their influence on an organization's ability to change (Waterman, Peters, and Phillips 1980). Specifically, we looked at the policies, processes, culture, technology, and physical environment within the Marine Corps' cyber workforce and their impacts on retention. These variables include both the transactional level of human behavior and the processes of organizational transformation, which Burke and Litwin (1992) describe as distinct sets of organizational dynamics that are required for genuine change in organizational culture. Participants' responses were manually inputted and recorded into a data collection spreadsheet utilizing Microsoft Excel. Grounded theory procedures outlined by Corbin and Strauss (1990) were followed to ensure thorough and accurate data collection was conducted. The process of sequential data collection and analysis was used to ensure potentially relevant information is identified as soon as perceived and to assist in the direction of subsequent discussions (Corbin and Strauss 1990). The research data was used to ensure concepts were recognized, categorized, and examined for patterns and variations (Corbin and Strauss 1990).

The categorized data and resulting concept themes were quantified by using frequency of responses to identify respondent patterns. The frequency of these themes were labeled "most" to indicate a majority of respondents (five or more) and "some" to indicate less than a majority of respondents (four or less). The frequency of concept themes also determined the rank of their perceived importance when approaching and listing them as input for phases three and four of this study.

B. THE DESIGN THINKING WORKSHOP

To support our investigation into non-monetary incentives for retention, we conducted a three-day workshop at the Naval Postgraduate School using the Design Thinking methodology. Participants were a mixture of practicing cyber professionals, cyber recruits and students, Navy Human Resources professionals and students, and human-centered design facilitators. Within the workshop, three teams independently explored the problem space. The workshop's theme was to explore opportunities to strengthen the DOD's cyber workforce. The intent was to generate ideas and develop initial prototypes for retention. The resulting prototypes were used as additional data for this study.

1. About Design Thinking

Design Thinking is a collaborative process of problem-solving that helps organizations innovate and create new alternatives for business and society (Brown 2009). Stanford University's Hasso Plattner Institute of Design, one of the leading academic institutions for Design Thinking, describes Design Thinking as a human-centered, prototype-driven process for innovation that can be applied to product, service, and business design (Cohen 2014). This process is characterized by specific problem-solving principles and includes a set of processes to support innovation.

2. Principles of Design Thinking

According to Salem (2014), Design Thinking is differentiated from other problem-solving practices by its integration of four essential practices: a focus on humans, a heavy use of prototypes, an iterative design/test process, and an emphasis on innovative processes and results.

First of all, Design Thinking focuses on humans within a system. Design Thinking looks at how humans think, feel, and act within a specific context of use. It strives to build an empathetic understanding of the problem space through empirical research that focuses on human needs and actions. Design Thinking is also a collaborative process that uses multidisciplinary design teams and integrates a broad

range of stakeholders—users, customers, and influencers. This human focus results in increased productivity, decreased errors, and decreased training and support costs (Bias and Mayhew 2005).

Secondly, Design Thinking uses models and prototypes, often basic in form, to encourage exploration, to support creativity, and to rapidly develop ideas. According to Brown (2008), “The goal of prototyping isn’t to finish. It is to learn about strengths and weaknesses of the idea and to identify new directions that further prototypes might take.” Prototypes are used to think about the problem space by making ideas explicit.

A third aspect of Design Thinking is the iterative exploration and testing of design ideas. Prototypes are used as disposable hypotheses, where initial ideas are mocked up in low fidelity forms so that design solutions can be made visible and tested. The prototypes increase in complexity and fidelity as design options are developed. Rapid prototype/testing cycles are known to speed up development time, lower development costs, and reduce the risk of product failures (Bias and Mayhew 2005).

Finally, Design Thinking emphasizes innovation. Innovation is not just inventing a new product or solution. Innovation is seen as both a solution type and a process. Innovative solutions are technologically feasible, have business viability, and are usable and desirable. Innovative solutions therefore require a design process that can operate in business time frames and can support human values. The Design Thinking process supports innovation by combining creativity with analytical thinking and by using lateral, generative processes rather than linear steps (Brown 2008).

3. Design Thinking Process

The Design Thinking process consists of multiple steps and is a way of systematizing innovation and creating new systems and processes (Pivot Learning Partners 2013). It typically consists of six steps: empathy, reframing, ideation, prototyping, testing, and iteration. Because of the time available, this workshop focused on the initial design phases and included only the first five steps—the process did not include testing or iterating on the initial design models. We did, however, include an

additional step by exploring data on the broad systemic factors impacting retention. The workshop process consisted of the following:

Systematizing: The workshop began with discussions on the interplay between Geopolitics, Economy, Diversity, Leadership, Technology Use, Informationalism, Attitude to authority, Work/Life Balance, Commitment, Work Structure, and Work ethos on the retention of cyber professionals in the DOD.

Empathizing: A key step in the Design Thinking process is to develop a deep understanding or empathy of the people and situations involved. The workshop provided two empathy explorations. The first exploration was a group interview of a panel of cyber professionals that included operators and human resources personnel both in and out of the Department of Defense. The second exploration was a presentation of the data collected in the initial interviews with Marine Corps' cyber professionals. Workshop participants were able to frame the problem using this information.

Ideation: Once the workshop participants had a deep understanding of the problem space, they were able to generate ideas for how to improve retention. Using brainstorming techniques and visual design processes, the participants created numerous design options.

Reframing: With several design options in hand, the participants discussed and prioritized the different options presented in their ideations. Taking parts from each, each group reframed the original problem statement to be more specific and actionable.

Prototyping: The final step in this workshop was the development of a prototype concept for retaining cyber professionals in the Department of Defense. The result was three initial conceptual models for improving retention.

Testing and iteration: Although not done during this workshop, the last steps in the design process include testing and iteration. Early models should be tested; based on the results, revisions should be made to the design. The process is then repeated until a viable and sustainable solution is reached.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESEARCH FINDINGS

Phases II and III of this study resulted in a set of qualitative data collected from initial collaborations and the design workshop. First, the retention information gathered during the in-person collaborations of Marine cyber personnel was categorized by theme. The frequency of response for each theme was then analyzed to determine its perceived level of importance to the respondents. As a result, eleven retention themes were identified, and then they were presented in phase III to assist in the design workshop process. The data collected from the workshop was then compared to the retention themes.

Based on the data gathered and analyzed during the collaboration phase, eleven themes emerged as considerable impacts to Marine cyber workforce retention. The themes included items related to incentives, personal factors, and organizational influences. Once these eleven themes were identified, they were incorporated into a Design Thinking workshop where the goal was to design conceptual prototypes for improving retention in the DOD cyber workforce.

Incentives

- **Monetary incentives**
- **Duty station preference**
- **Geographic stability**
- **Education**
- **Transferrable skills and external career opportunities**
- **Internal career progression**

Personal Factors

- **Personal interests and goals**
- **Culture and relationships**

Organizational Influences

- **Access to technology**
- **Process development**
- **Command climate and bureaucracy**

Prototype Solutions

- **Career progression model—where experts are developed**
- **Closed model—where everyone is a Cyber Warrior**
- **Fluid career model—where there are multiple pathways in and out**

A. INCENTIVES

The data from this study indicated that there are three types of incentives operating in the USMC Cyber workforce: monetary incentives, non-monetary incentives, and task or goal incentives.

1. Monetary Incentives

Money matters...period. Although much of the background research presented in this study explored the importance of non-monetary incentives on retention and their particular influence on the cyber workforce, this study found that monetary incentives do have a significant impact on the target population. In fact, every respondent in the collaborations mentioned the importance of competitive monetary incentives in some way. Whether in the form of cash bonuses, incentive pay, or the fact that higher salaries can be found in the private sector, most respondents felt that monetary incentives are a key factor in increasing retention within the Marine Corps' cyber workforce. As one Marine participant put it, "Money makes the world go around." Responses, however, did differ with respect to the actual value that monetary incentives created for the individual. This data reflected similarities with findings from previous studies on intrinsic motivations.

Traditional monetary incentives were repeatedly mentioned by the participants of this study. Most respondents felt that increased bonuses and incentive pays are required in order to compete with higher salaried private sector cyber security jobs. Because of the

current high demand for the unique skills cyber professionals receive, some respondents felt they should gain critical skills designation making them eligible for incentive pays like Special Forces Operators and military pilots. One Marine stated, “Bonuses are important when there is a vacuum in the private sector, especially when we’re making them [Marines] competitive in that environment.” In terms of higher salaried civilian positions, another respondent noted the challenges that are faced when competing with the private sector, “Once Marines know [about higher salaries], we have a hard time competing.”

The design process workshop also reiterated the need for competitive monetary incentives. Many participants felt the allure of better pay in the private sector is a challenge that the military will consistently have difficulty in competing. One civilian cyber security professional interviewed as part of the design workshop stated, “You must make it worth their while to stay. There’s a gold rush in cyber security in Silicon Valley right now.”

a. Monetary Incentives Are Not Sufficient

Though every participant in this study mentioned monetary incentives as a key factor in retention, all responses were not positive. Some collaboration respondents felt that the bonus money was not necessarily attracting or being offered to the correct people to improve long-term retention rates. With Zones A and B Cyber Security Technicians receiving some of the highest SRB rates in the Marine Corps, some respondents felt that initial lateral movers within those career zones may simply be attracted to the money offered before they understand what the job actually entails. The individuals that have the experience and requisite skills to be efficient in the cyber workforce are not receiving the same level of incentives. Responding to the lower SRB rate for senior Cyber Security Technicians, one respondent stated, “You need to give the money to the right people with the right skills.” Further, the bonuses are offered to individuals prior to processing their requisite security clearances or determination of skill aptitude for the job. Some respondents indicated it was not uncommon for Marines who had recently lateral moved into the cyber community, and received the SRB, to be forced to wait several months for

their security clearances to process or begin any prerequisite training within their respective units. Meanwhile, their reenlistment obligation has already begun, and they are unable to perform the specific duties with their reenlistment. As one Marine who was still awaiting a security clearance after several months at his command put it, “My clock is ticking here.”

This study also found that participants recognized the lack of intrinsic motivation monetary incentives provide. One workshop cyber professional said, “Money is not the key. People are seeking excitement and enjoyment.” Another Marine respondent stated, “Bonuses aren’t going to cut it if people aren’t content.” In addition, since officers are not offered retention bonuses in the Marine Corps’ cyber community, it was evident that monetary incentives played a much smaller role in their retention decisions. A pattern emerged in the study that showed most respondents and workshop participants believed a mix of extrinsic and intrinsic motivators are necessary to provide the adequate job satisfaction that would assist with long-term retention.

2. Non-monetary Incentives

When looking at what motivates Marines to stay in the cyber force, we discovered four areas that impacted their decision. The participants noted that duty station preference, geographic stability, education, transferrable skills, and external career opportunities were all important decision factors in retention.

3. Duty Station Preference and Geographic Stability

Where one works makes a difference. This is true for both original duty station assignments and in maintaining geographic stability. Duty station preference and geographic stability are similar but not the same. Preference is considered one tour of the Marine’s geographic choosing. Geographic stability, often referred to as homesteading, is two or more consecutive tours. Geography plays a role in supporting quality of life for families in terms of spousal careers and education as well as continuity for their children’s education.

Data collected from participants shows that both duty station preference and geographic stability are a strong retention factor for Marines, specifically. An available position at the desired duty station is required for a Marine to move there. Without an open position, the desired duty station is unattainable. In addition, if a Marine wants geographic stability, then another Marine that desires to go to that position cannot. The Marine Corps' attempts to balance desires and needs accordingly, but the data indicates that a Marine's preference and the needs of the Marine Corps do not always align.

a. Duty Station Preference Matters

The Marine Corps has a four-year tour requirement for Marines stationed at MARFORCYBER. The four-year requirement is in place to allow for minimum return on investment from its Marines stationed there. Marine participants said that after this four-year tour, cyber operators are often sent back to fleet units. This is due to the high value placed on deployments and “fleet time” for promotion and rotation purposes within the Marine Corps. Major commands, such as a Marine Expeditionary Force (MEF), do have requirements for cyber security specialists, but these requirements often do not require the technical level of MARFORCYBER-trained operators. As a result, the MEFs receive highly trained personnel that are underutilized. As one Marine stated, “It’s a waste when we are sent back to the fleet.” This waste of talent is due to the MEF’s reliance on using cyber workforce Marines primarily in an administrative role—maintaining records or keeping up with paperwork for inspection purposes. The Marine’s skill set then atrophies from underutilization. Most cyber personnel considered this overemphasis on “fleet time” an “old way of thinking” and found it limited their willingness to remain on active service.

b. Geographic Stability is Important

Stability matters. Marine participants stated that they wanted to remain in a relevant cyber-role where they can use their skills. Cyber personnel receive intrinsic rewards by participating in the uniquely challenging arena of cyber security. The main hindrance to stability is the effect of remaining at a cyber-command, which is viewed negatively by promotion boards as a non-operational unit. Participants mentioned their

desire to remain in their cyber security roles by stating their desire to “allow back-to-back cyber assignments without hurting my career.” Cyber personnel want to hone their skills and utilize them to face the challenges presented in the cyber world: This is where they derive a significant amount of their intrinsic motivation. Most participants felt that it is a “waste” and “inefficient” to be removed from the cyber “Meccas.”

Families benefit from stability, too. Those with spouses want to live in areas that provide the best prospects for spousal career or education opportunities. Stability provides the spouse an opportunity for career growth and the opportunity to finish education. Stability also impacts those with kids who have to remove them from school, if ordered to relocate, after they have established friendships and continuity in their education. A few Marine participants made statements about the importance of their and their spouse’s education and the positive or negative impact of either having the opportunity to stay at a duty station or leave.

4. Education

Cyber personnel value education and training opportunities so they can sharpen their skills and earn valuable certifications. The private sector, by and large, requires a college degree for employment in cyber security, and this is one reason why cyber personnel pursue them. As one Marine stated, “Most of the high paying jobs require a degree.” Certifications and training that are received on the job are also transferable into college credits toward computer science or information technology (IT) fields. The Marines earning degrees also sought a college degree and additional training as a personal goal. The additional training is appreciated by Marines because it helps advance their career and their skills. Education is often viewed as a reward. The Marine Corps, for its part, encourages Marines to further their cyber education if it is relevant and beneficial to the mission. Training, however, is a double-edged sword. The certifications earned through training are valued in industry and increase the marketability of the individual.

5. Transferrable Skills, Experience, and External Career Opportunities

The military cyber education process makes DOD cyber personnel more marketable because the required training for the cyber workforce parallels that of the

private sector. Additionally, the top-secret security clearances held by these personnel command a high value. Education and security clearances are recognized as keys to getting cyber jobs and every Marine respondent understood the availability of higher paid private sector jobs. In fact, civilians are being hired to fill active duty vacancies, which have created somewhat of a revolving door. Marines frequently get out of active duty and then get hired as GS employees in essentially the same roles for more money. Participants noted that this practice does not seem to have a negative internal impact. The benefits of having a GS position (as opposed to an active service position) are: Marines typically do not have to PCS; they will most likely not deploy; there are no physical fitness requirements; and there are relaxed grooming standards. Participants, however, noted that this revolving door may be short-lived due to the potential for decreasing demand once the workforce reaches equilibrium in a few years.

Most participants felt the cyber education and experience that was available to them in the Marine Corps would help them in their future job searches. One respondent commented on the challenges of finding desirable work in the civilian sector: “Most of the high paying jobs now require a degree *and* experience.” Another Marine noted that work experience was important even in low skill technical jobs, “Even the Geek Squad wanted one year of experience and they are only paying nine dollars an hour.”

6. Internal Career Progression

Our discussions with cyber personnel in the Marine Corps indicated that four factors were important to them when looking at the progression of their careers. First, Marines want the opportunity to do what they are trained to do. Second, they want to have a career roadmap. Third, they want to eliminate barriers to promotion. Finally, they want stronger role for personnel in middle management positions.

a. *Career Opportunities are Desired*

Participants indicated that career opportunities such as rank, skill development, and billets are important to them. Some of the discussions revealed that promotions were important in both attaining more responsibility and earning higher pay. What seemed equally important to promotions were the development of new skills and the opportunity

to earn additional certifications such as Certified Ethical Hacker. Additionally, Marines placed an emphasis on wanting the opportunity to utilize their skills and training operationally. As one Marine stated, “I want the opportunity to do what I was trained for.”

b. Career Roadmaps are Needed

Both the officers and enlisted Marines that we interviewed expressed frustration with the lack of adequate career roadmaps. A career roadmap outlines important career milestones so a Marine knows what is required for promotion in a particular career field. Most participants expressed misgivings about the absence of developmental standards for their profession. The current career roadmaps for enlisted personnel were described as “inadequate” while officers and warrant officers said their roadmap was “nonexistent.” Additionally, the roadmaps have not kept pace with the changes in the cyber community. As a result, the communication of expectations between the policy makers and the operators is insufficient.

c. Barriers to Promotion Reduce Retention

As noted earlier, participants expressed the desire for back-to-back tours at their cyber-related commands without impacting their chances for promotion. As one Marine participant stated, “I just want to stay in my cyber job without it hurting my career.” The military places more value on traditional operational roles and cyber commands are not viewed in the same light as operational activities. As a result, even though cyber professionals may remain at their jobs, their Marine Corps’ careers are affected negatively. Officers were especially frustrated because promotion boards do not currently value the time spent at cyber commands that are outside of their primary MOS. One Marine had an especially noteworthy comment from a monitor, or career counselor, who stated that remaining at a cyber-command will, “Ruin your career.” Along those same lines, several respondents’ comments took the form of, “This is where people come to retire.” Many of the participants questioned the impact of career policies on retention, noting the disparity between the retention problem and current policies that essentially pushes Marines out by not valuing time spent at cyber commands.

d. Absence of Middle Management Limits Growth

Junior enlisted and non-commissioned officers have little opportunity to learn typical military leadership skills such as mission planning briefing. In traditional units, these personnel are involved in such mission planning activities and will eventually have the experience to lead their own planning sessions and briefings. Participants discussed the absence of middle management as a root cause of this shortcoming. There is currently an imbalance of ranks, where higher ranking personnel fill junior roles. One officer mentioned that this was the result of “captains filling the roles of lance corporals because of the top-heavy staff.”

B. INTRINSIC MOTIVATORS

The importance of intrinsic motivations within the cyber workforce became apparent early in the collaborations and was substantiated during the design process of this study. Most participants mentioned one or more intrinsic motivators that were consistent with previous research. This study found that intrinsic motivators were influenced by the individual’s personal factors and the organizational influences he or she encountered.

1. Personal Factors

According to most study participants, individual factors played an important role in influencing their retention. These factors were derived from personal interests and goals, as well as the culture of the cyber workforce and the personal relationships within it.

a. Personal Interests and Goals Influence Retention

Like much of the background research on intrinsic motivation, this study also found a link between retention and personal interests and goals. Pre-existing interests in technology, the allure of cyber work, the career stage, and alignment with the mission of the Marine Corps are all significant motivators.

First, most participants described how pre-existing interests and their experiences in IT impacted their desire to be in the cyber field. Not only is the job interesting to them, but the subject matter is something that many pursue on their own time. They pursue this through formal education and personal hobbies. For example, some Marine respondents were actively pursuing degrees in the IT field, and most of the civilian cyber professional workshop participants already held IT degrees. In addition to education, most participants admitted to having IT-related hobbies or participating in IT-related events outside of the work environment. These activities included studying to keep pace with current technology, building or troubleshooting personal computers, creating software, and of course gaming. One Marine noted how cyber interests carry over from their professional to their personal lives, “These guys leave work and go home and play video games with each other.” Regarding the studying required to ensure their knowledge remains current, another participant said, “I’m forced to research on my own to stay ahead in both my job and personal life.”

Second, most participants cited the allure of a cyber career as a motivator to remain in the cyber workforce. The opportunity to work at a cyber command appeared by itself to be an intrinsic motivator for most cyber personnel.

A third personal factor impacting individual goals is the age or career stage of the cyber employee. Younger and less experienced participants cited increased responsibilities as well as a desire to learn new and exciting skills as their primary goals within the cyber workforce. More senior and experienced participants mentioned job security and retirement as goals; however, they caveated these influences with the fact that private sector jobs are still alluring. One Marine alluded to the attraction of the private sector by stating, “Even after thirteen years [of military service], I’m still weighing my options.”

The fourth retention factor that surfaced was the importance of a shared mission. One respondent specifically cited the responsibility that comes with the cyber role in the military, “Working in the military aligns with my goals. It’s fulfilling and gives me more responsibility.” Most participants agreed there was a level of congruence between their personal goals and the organization’s goals. One Marine said, “Everyone is focused on

the same mission and goals.” Most participants applied to enter the cyber field. As a result, most participants identify with the importance of their job and align themselves with the organizational goals. Additionally, a sense of mission and purpose from their work was mentioned by most participants. These intrinsic motivators were described by one Marine as, “Above just coming to work.” While most of the participants felt these factors were positive, some actually mentioned their potential barriers to retention. If Marine cyber personnel are forced to move into less challenging positions or begin to feel stagnant, they may be forced to branch out to achieve their goals. As one Marine put it, “The same things attracting them to this job, are the same things that drive them out.”

2. Cyber Culture and Relationships

The culture—the shared practices, knowledge, beliefs, values, and attitudes of a group—are extremely important to the cyber community. Most participants had a distinct sentiment that the cyber workforce is a unique population. They described themselves as “intelligent” and “different,” and one participant even stated, “We’re the cool kids on the block.” All the participants voiced their appreciation for the culture, and they mentioned the positive impact it has on the cyber workforce. This study found that cyber professionals felt their job was intriguing and challenging. One of the most important aspects mentioned was what both Marines and civilian cyber professionals described as an “environment of learning.” This learning environment provides opportunities for them to challenge themselves intellectually and remain engaged in their work. Intellectual engagement was identified as a key factor in attracting and retaining cyber personnel. As one person noted “smart, technical, and independent individuals who are motivated to learn,” are essential for a quality cyber team.

This study also found that the culture of the community impacts the types of relationships that cyber professional’s desire. While most cyber professionals enjoyed the challenging and competitive work, they also expressed their appreciation for a collaborative and social environment. Respondents described a sense of teamwork that influenced them to work together to solve problems and learn new skills. Most participants felt they worked with individuals who were like-minded and shared the same

interests and goals. Referencing the fact that Marines request to lateral move into cyber-related occupation specialties, one Marine pointed out, “We all chose to be here.” Some participants described their coworkers as “peers” who were focused and genuinely interested on the cyber mission. Describing the peer relationship among cyber professionals, one respondent stated, “Everyone brings something to the table. There are no egos here.” This teamwork coexists with a sense of friendly rivalry. One participant described the competitive nature among them as having a positive impact on problem-solving, “They want to impress others with their technical prowess.”

This study further found that most participants felt there was a clear difference between the cultures of the cyber community and the Marine Corps in general. Interestingly, most respondents did not feel that these cultural differences alone were a significant barrier to retention. Some even mentioned their pride as Marines was a further intrinsic motivator to remain in service. Most respondents, however, described organizational influences as more of a factor that impacted these differences and posed a significant challenge to retention of cyber personnel.

C. ORGANIZATIONAL INFLUENCES

Just as personal factors are important for cyber personnel, the organization itself offers a variety of intrinsic motivators that influence retention. The organizational influences that emerged as themes in this study related to the access to technology, process development within the cyber community, and the command climate and bureaucracy of the organization.

1. Access to Technology

Technology was found to be a significant motivator for most cyber personnel. This study, however, found there were distinctly different outlooks on whether it was a positive or negative influence within the Marine Corps’ cyber workforce. Much of this was based on individual roles and responsibilities, which was primarily dependent upon experience and seniority. Most younger, less experienced cyber professionals referred to the technology as “new” and “cool” and commented on “exciting access to new capabilities.” Most of these individuals felt they currently had access to the “latest and

greatest” technologies. In addition to this technology is the inherent training required to effectively utilize it. Some respondents commented how the technology and training combined as a motivational tool, “I’m actually using the gear I was trained on,” said one. Another stated, “I get to work with and do things here I won’t do anywhere else.” In contrast, older, more experienced individuals had a different view of the current state of the technology and how it negatively influences retention decisions. They noted the defense sector is very specific and directive on what is allowed to be used. Most of these respondents described equipment and technology as “limited” and “archaic.” A DOD civilian cyber professional interviewed as part of the design workshop stated, “We’re dealing with antiquated systems because of our [acquisition] constraints.” Most of the experienced participants described this perceived lag in technology within the USMC and DOD as a primary challenge to retention. In comparison to the private sector, one Marine said, “There’s so much more out there. We’re competing with an industry model with the latest software and next generation technology.” A civilian cyber security professional corroborated this perception of the civilian sector by stating, “The industry is constantly changing and morphing our capabilities.” Study participants further described the desire to work with cutting edge technology as an influence to depart service. As one Marine put it, “They see the outside as the ‘sexy’ cyber workforce. Once they realize we’re deficient, they leave for more hands-on tech jobs.”

2. Process Development

Most participants described a sense of involvement in developing new processes within the cyber workforce as another influential motivator. This organizational involvement aligned with previously described personal factors such as a sense of purpose and empowerment. Most participants explained how the innovative and evolving nature of the cyber workforce are attractions towards the field. One Marine respondent described the process development within the cyber community as, “It’s exciting to break new ground. We’re actually writing the book here.” Another explained they are creating doctrine and are now widely considered the resident experts in their field within the Marine Corps, “They look to us for the answers. If we don’t know it, nobody does.” Most participants, however, also noted that the evolving nature of the cyber community has

created some resentment about the lack of alignment with USMC and DOD policies and processes. Both Marine respondents and DOD civilian participants described “antiquated” government processes (such as acquisitions and human resources) as major challenges. According to participants, these processes do not align with the rapid technological advancements that the cyber workforce requires. Regarding the time requirement for system acquisitions, one respondent stated, “The procurement process is limiting our progress. It wasn’t meant for this type of technology.” Both military and civilian respondents also described the time requirements for general military instruction and annual training of personnel. One DOD civilian described the challenges he faces with military staff in his department, “I can only plan to utilize them 60 to 70 percent of the time. The other 30 percent is taken up with their military requirements.” A Marine respondent mentioned the challenge of balancing a Marine’s promotion training requirements and cyber training requirements, “We need to better allocate our time. Some of these Marines are more proficient at shooting a rifle than they are at these systems.” Another described the challenge of dealing with the lack of sufficient personnel due to these training requirements, “Who’s monitoring the networks? If they get over tasked it can be discouraging.”

3. Command Climate and Bureaucracy

Lastly, a theme that often arises when considering organizational impacts in the military is that of command climate and bureaucracy. Contrary to previous retention research, this study found that most respondents did not feel that the command climate was weak or that bureaucracy was a major impediment. In fact, most Marine respondents spoke positively of the command climate they experienced. Marines described the climate as “open,” “collaborative,” and “innovative.” They noted that leadership openly pushes creativity and training and is “mission-focused.” Most felt they were a “high priority” because of their cyber mission. In describing the impact of the climate on new personnel, one respondent stated, “Once here they realize the grass is, in fact, greener. The more training, the more impact (they make), the less they want to leave.” Only one respondent described minor frustration with the bureaucracy of the job, “Because we’re relatively new, it causes some confusion. We get drug [sic] in different directions a lot.”

Most participants, however, admitted it was not a significant organizational influence on retention. One Marine took a practical approach to the bureaucracy by stating, “We have to get approval to do everything, but that’s to be expected. Besides, every job will have some sort of approval process.”

D. PROTOTYPE SOLUTIONS

As a result of the Design Thinking workshop, three retention prototype models were developed: a career progression model, a closed system model, and a fluid careers model. The three prototypes have common themes:

- Focus on increasing the pool of recruits
- Be transparent in setting expectations
- Hire for “good fit”
- Support progression of skills
- Adapt to changing demographics
- Use flexible incentives
- Support movement in and out of military
- Modernize human resource processes

1. Career Progression Prototype—Experts are Developed

The career progression prototype starts with attracting personnel and managing expectations through transparency. Personnel will know what to expect from going into the cyber field. The career path and training are communicated to potential recruits so they know what to expect in terms of progression, training, and certifications. This model assumes differences in motivation for early career individuals and mid-to-late career individuals. Potential recruits are filtered by knowledge, aptitude, attitude, and motivation. Early career individuals are focused on building their skills and attaining certifications. While building skills and earning certifications, the individual will rotate through the cyber functions—support, offense, and defense. Merit-based opportunities,

such as special assignments for the National Security Agency (NSA), internships with industry partners, or Naval Postgraduate School (NPS) attendance are offered to those with exceptional skills. These assignments are tied into service commitments that ultimately bring them back to building skills in support, offensive, and defensive operations.

Mid-to-late career personnel are assumed to pursue job stability, competitive salaries, and have family considerations. Additionally, mid-to-late career people are assumed to take on supervisory, managerial, or leadership roles. During this time they will build their management skills and solidify their positions as resident experts. Since these personnel are resident experts, special attention is paid to their retention. As a result, sabbaticals may be offered. These sabbaticals may include professorships at higher learning institutions such as NPS or opportunities to give back to the community.

2. Closed prototype – Everyone is a Cyber Warrior

The closed prototype requires the establishment of a sustainable DOD personnel supply chain and leverages the competitive nature of cyber professionals. A sustainable supply is established by developing programs inside of the general education system that teach computer science. Inside the DOD, pilot programs are established in JROTC and ROTC programs. Once in the active military, cyber individuals are placed into tiers. Each tier, one through four, has varying individual skill levels. Tier one is the baseline and everyone, DOD-wide, will attain tier one status. For example, tier one personnel will have the requisite skills to perform their own troubleshooting without the need for technical support. To progress into the more advanced tiers, an individual must compete against higher tier personnel to prove skill level. Tier four are the most highly trained—the cyber police—and they develop exercises for teams to compete against each other internally within the DOD as well as externally to industry partners that compete for DOD contracts by winning the exercises.

3. Fluid Career Prototype—Pathways In and Out

The fluid career prototype focuses on the inevitability of change. It first utilizes modern recruiting methods and outreach programs to “seed the pool” to build the

potential labor market. Modern recruiting techniques such as cyber defense challenges (“Honeypot” challenge) or other puzzles and shooting games are used. Outreach programs such as STEM (the academic disciplines of science, technology, engineering, and mathematics) and other methods are used to expose diverse groups of people to the sciences and thereby expand the pool of potential recruits. Entrance into the cyber workforce is done through a thorough evaluation and alignment of skills with mission goals. Strategic goals and return on investment drive quotas for cyber employees. Recruits are matched with mission by assessing potential personnel by personality, aptitude, career goals, skills, knowledge, and training. Encouraging rotations through the various roles—support, defense, attack, management and innovation—grows the force. The cyber workforce is also supported and incentivized by allowing flexible work schedules, exceptions to policy, and on-going skill growth. Throughout the career pathway, there are adjustments for change and growth (personal, organizational, and national). These adjustments include exit ramps and on ramps where personnel can move between active service, reserves, civilian, and industry jobs. Each exit and on ramp represents opportunities to leave the service and to re-enter the service fluidly.

The above prototypes are only a first step in designing solutions to the retention of cyber employees as defined in the “methodology” section of this study. These findings provide insight into the core issues surrounding retention troubles for the Marine Corps’ cyber workforce. The findings show that the retention issue is deeper than financial incentives; alternative solutions that nurture intrinsic compensation are vital to the success of any future cyber retention program.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

The purpose of this study was to identify and analyze critical factors that cause Marine Corps' cyber workforce personnel to separate from active service and explore opportunities to strengthen retention strategies. This study utilized collaborations with operational Marine cyber personnel and a Design Thinking workshop to generate ideas and develop initial prototype solutions for retention. The data collected is intended to support on-going efforts to resolve the challenges in retaining high value personnel.

According to the DCWS (2013), cyberspace is a mission critical warfighting domain facing critical personnel shortages that could impact operational readiness. The DOD and Marine Corps have placed a premium on their cyber capabilities in recent budget cycles. Retention challenges of cyber personnel, however, are still an issue. The impacts to the military's cyber retention goals include: increased competition with the civilian sector, reduced budgets, a small labor pool of cyber professionals, and the unique characteristics and desires of these individuals. This study identified numerous themes that are important to Marine cyber personnel and other cyber professionals. These themes were individually explored to find their significance and value to these highly specialized workers.

An acute understanding of extrinsic and intrinsic motivations is required when analyzing the value of incentives to cyber personnel. These motivations are further influenced by the unique characteristics and interests of cyber personnel. While the use of monetary incentives as extrinsic motivators is a concept traditionally used in military retention, it does have limitations. These incentives may not be sustainable during fiscally and politically constrained times. Further, this study aligns with previous studies to conclude that intrinsic motivators are important to cyber professionals. The cyber workforce culture has been characterized as "intellect-centric" (Conti and Raymond 2011) and comprised of independent, creative, and technical individuals. These individuals place more value on technology, knowledge, intellectually challenging tasks, and meaningful work with a sense of purpose. While compensation is highly important to

cyber professionals when considering overall quality of life, it is not one of the most important factors when considering a job (Semper Secure 2013).

This study concludes that a tailored approach to retention must be considered. The personal and organizational influences that were uncovered in our study support the importance of a mixed approach. We show that retention factors vary greatly by individual situations. The identified retention themes can serve as either a positive or negative influence, dependent upon the individual. A robust and tailored cyber retention strategy, that includes include both extrinsic and intrinsic motivators, would allow the Marine Corps to emphasize the important commitment it has to its cyber personnel and to create an environment that is attractive to these highly skilled cyber warriors.

A. KEY STAKEHOLDERS AND THEIR INVOLVEMENT

When looking to improve cyber retention, special care must be taken to involve key stakeholders since they stand to gain or lose from the success or failure of cyber retention. Satisfying key stakeholders is critically important in achieving the desired outcome and retaining cyber personnel (Bryson 2004). Stakeholder engagement may serve two purposes. First, information gained from the engagement may help create an appropriate solution to the retention problem. Second, stakeholder engagement helps in creating buy-in after a potential solution or solutions are developed (Boutelle 2004). Although we were not able to completely flush out the characteristics of all the stakeholders, key influencers in the retention of Marines in the cyber workforce include individual Marines, MARFORCYBER, and the Marine Corps.

1. Individual Cyber Marines

The individual Marine is the most critical stakeholder in retention. As the end users of any retention policy, Marines serve as evaluators of the strengths and weaknesses of any proposed system. The ultimate evaluation, of course, is derived by Marines choosing to stay or leave active service. The policies used to keep their skill sets will either create value—and convince them to stay—or drive them out. A Marine's power to influence policy is derived from this ability to leave the organization for an opportunity to better pursue goals and personal interests (Bryson 2004). This ability to leave requires

that the Marine Corps pay attention to the individual cyber Marine's unique needs and desires. Marines in the cyber security field want to stay actively involved in their field at a command where their unique skills are utilized and where growth opportunities exist. Cyber Marines want to continue to take part in the unique mission set and opportunities associated with a relevant cyber command.

2. MARFORCYBER

MARFORCYBER needs to retain qualified personnel who have the skill sets to achieve its critical mission objectives. In other words, their mission relies on people; these people are in short supply. Additionally, retaining key leaders that have the requisite skills to understand and manage the cyber operator is critical in achieving mission success. MARFORCYBER may measure success of retention practices by its ability to accomplish mission objectives effectively.

3. The Marine Corps

By retaining cyber personnel, the Marine Corps will better achieve its cyber mission in support of national objectives. As an influencer, the Marine Corps has a voice on Capitol Hill and may have to solicit action at the congressional level for new measures and powers to retain personnel. Measures such as incentive pay require congressional action. The Marine Corps may measure success by filling manpower staffing goals and accomplishing national policy objectives.

B. RECOMMENDATION

This study has to take into account the feasibility of its implementation. Simply stating “provide higher monetary incentives to cyber personnel” or “improve the acquisitions process of cyber security technology” do not provide significant and actionable feedback to stakeholders. Therefore, our recommendations focus on policy considerations and how they align with the focus areas outlined in the DCWS.

This study recommends that the Marine Corps consider tailoring its current promotion and Time On Station (TOS) requirements to the unique needs of the cyber

workforce. These organizational policies are described as “the old mindset” by some participants, and they are looked upon negatively by most cyber personnel. These policies do not support the specialization of the cyber community and the intrinsic motivations they seek. For example, most participants had a strong desire to remain at a cyber command, utilizing their training and technical abilities in a direct role. This desire was directly tied to themes such as personal goals, career progression, and duty station preference; however, a typical promotion board would look negatively upon too much time at one command. The specialized training cyber Marines receive requires significant time and resources; therefore, the return on investment of traditional rotation policies should be closely examined. Additionally, the “old mindset” or “check-in-the-box” approach to career progression is insufficient for the cyber workforce as it often pulls Marines into non-MOS specific billets. This has a significant impact on the technically skilled individuals of the cyber workforce due to rapid skill atrophy as technology advances. Marine cyber personnel are a valuable commodity in a limited market and must be afforded the opportunity to remain in positions to utilize their skills without harming their careers or indirectly creating disincentives to retention.

This recommendation is in line with critical elements outlined in the DCWS Focus Area 4, and it is consistent with this study’s focus on intrinsic motivations and non-monetary incentives.

C. RECOMMENDATIONS FOR FURTHER RESEARCH

Further research is recommended to more accurately define and approach the issue of Marine Corps’ cyber workforce retention. Possible topics should include:

- First, quantify the cyber retention challenges currently faced in the Marine Corps. Retention of Marine cyber personnel should be measured against other critical MOSs and other service component’s cyber personnel to accurately determine the state of the problem faced. This must be achieved to be able to effectively measure the success of any retention program or policy implemented.

- Second, better define the cyber roles which are targeted for retention and also what required skills make them attractive. This would allow a more comprehensive tailored retention strategy for those individuals of higher value to the organization.
- Third, research existing exit briefs (or conduct them if necessary) of departing cyber workforce personnel to identify precise motivations for their departure from service. A larger and more diverse study population is needed to achieve findings that determine more robust variances in retention motivators.
- Finally, further testing and iteration of retention prototypes are needed to achieve the viable and attainable solution desired through the Design Thinking process. These iterations should include the identified stakeholders at all levels of the organization, including policy makers.

D. FINAL WORDS

Human capital is the key component in the Marine Corps' mission to expand its cyber capabilities. The highly trained and technical individuals that make up the cyber workforce are limited and highly sought after in defense of our Nation and enterprise. As the Marine Corps expands its warfighting capabilities in the cyber domain, it will require a unique approach towards a unique group of Marines with unique characteristics and needs. Implementing a strategy that uniquely responds to these cyber warriors will ensure mission success.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. COLLABORATION QUESTIONS

DISCUSSION POINTS

- **What things influence a cyber professional to join the Marine Corps?**
- **What things influence a cyber professional to stay in the Marine Corps?**

FOLLOW UP QUESTIONS

- **How do USMC cyber workforce policies impact retention?**
- **How do USMC cyber workforce processes impact retention?**
- **How does the USMC cyber workforce culture impact retention?**
- **How do USMC cyber workforce technologies impact retention?**
- **How does the USMC cyber workforce physical environment impact retention?**
- **In a perfect world, what would you do to improve retention in the USMC cyber workforce?**

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Anderson, Sharon. 2013. “Recruiting, Training, and Maintaining Talent in the Cyber Workforce.” *CHIPS: The Department of the Navy’s Information Technology Magazine*. <http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=4727>.
- Alexander, Keith B. March 12, 2013. *Statement before the Senate Committee on Armed Service, 2013*. 113th Congress. http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf.
- Asch, Beth J., Paul Heaton, James Hosek, Francisco Martorell, Curtis Simon, and John T. Warner. 2010. *Cash Incentives and Military Enlistment, Attrition, and Reenlistment*. Santa Monica, CA: RAND National Defense Research Institute.
- Bassett-Jones, Nigel, and Geoffrey C. Lloyd. 2005. “Does Herzberg’s Motivation Theory Have Staying Power?” *Journal of Management Development* 24(10): 929–943.
- Boutelle, Jonathan. 2004. “Understanding organizational stakeholders for design success.” Paper presented at Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques, ACM Press New York, NY, USA.
- Bryson, John M. 2004. “What to do when stakeholders matter: Stakeholder identification and analysis techniques.” *Public Management Review* 6(1): 21–53.
- Bias, Randolph G., and Deborah J. Mayhew, eds. 2005. *Cost-Justifying Usability: An Update for an Internet Age* (Morgan Kaufmann Series in Interactive Technologies). Burlington, MA: Morgan Kaufmann, an Imprint of Elsevier.
- Brown, T. 2008. “Design Thinking.” *Harvard Business Review* 86(6): 84–92.
- Brown, T. 2009. *Change by Design. How Design Thinking Transforms Organizations and Inspires Innovation*. New York, NY: Harper Business.
- Browning, Amanda G., and Clinton F. Burr. 2009. “Monetary and Non-monetary SWO Retention Bonuses: An Experimental Approach to the Combinatorial Retention Auction Mechanism (CRAM).” Master’s thesis, Naval Postgraduate School.
- Bureau of Labor Statistics, U.S. Department of Labor. October 9, 2014. *Occupational Outlook Handbook, 2014-15 Edition*. Information Security Analysts. <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm> .
- Burke, W. Warner, and George H. Litwin. 1992. “A Causal Model of Organizational Performance and Change.” *Journal of Management* 18(3): 523–545.

- Charmaz, Kathy. 2006. *Constructing Grounded Theory: A Practical Guide Through Qualitative Research*. London: Sage Publications.
- Chief Information Officer. December 4, 2013. *Department of Defense Cyberspace Workforce Strategy*. Washington, DC.
http://dodcio.defense.gov/Portals/0/Documents/DoD%20Cyberspace%20Workforce%20Strategy_signed%28final%29.pdf.
- Cohen, Reuven. 2014. “Design Thinking: A Unified Framework for Innovation.” Forbes Online. <http://www.forbes.com/sites/reuvencohen/2014/03/31/design-thinking-a-unified-framework-for-innovation/2/>.
- Cole, Alexandra L. 2014. “U.S. Marine Corps Enlisted Retention: An Analysis of Stakeholder Incentives for the Retention of Tier 1 First-Term Marines.” PhD dissertation, Monterey, CA: Naval Postgraduate School.
- Conti, Gregory, and David Raymond. 2011. “Leadership of Cyber Warriors: Enduring Principles and New Directions.” *Small Wars Journal*.
- Corbin, Juliet, and Anselm Strauss. 1990. “Grounded Theory Research: Procedures Canons and Evaluative Criteria.” *Qualitative Sociology* 13(1): 3–21.
- Coughlan, Peter J., William R. Gates, and Noah Myung. 2013. “One Size Does NOT Fit All: Personalized Incentives in Military Compensation” (No. NPS-GSBPP-13-002). Monterey, CA: Naval Postgraduate School.
- Coughlan, P., Gates, W., and Myung, N. 2013. “The Combinatorial Retention Auction Mechanism (CRAM).” Unpublished manuscript. Monterey, CA: Naval Postgraduate School.
- Crouch, M. and H. McKenzie. 2006. “The Logic of Small Samples in Interview-Based Qualitative Research.” *Social Science Information* 45(4): 483–499.
- Defense Finance and Accounting Service. 2013. “Military Pay Table.”
<http://www.dfas.mil/militarymembers/payentitlements/militarypaytables.html>. Dec 31, 2013.
- Department of Defense. 2011. *Cyber Operations Personnel Report*. Report to the Congressional Defense Committee. Washington, DC. <http://www.nsci-va.org/CyberReferenceLib/2011-04-Cyber%20Ops%20Personnel.pdf>.
- Department of Defense. 2012. *Report of the Eleventh Quadrennial Review of Military Compensation*. Washington, DC: Office of the Secretary of Defense.
- Department of Defense. 2014. *2014 Quadrennial Defense Review*. Washington, DC: Office of the Secretary of Defense.

- Glaser, Barney G. and Anselm L Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Transaction.
- Harrison, Todd. 2012. *Rebalancing Military Compensation: An Evidence-Based Approach*. Center for Strategic and Budgetary Assessments.
- Kapp, Lawrence. 2013. *Recruiting and Retention: An Overview of FY2011 and FY2012 Results for Active and Reserve Component Enlisted Personnel*. Washington, DC: Library of Congress Congressional Research Service.
- Lesser, Evan. 2013. “2013 ClearanceJobs Compensation Survey: The Great Rebalance.” http://www.clearancejobs.com/files/security_clearance_compensation_2013.pdf.
- Lesser, Evan. 2014. “2014 In the Clear: Compensation Decline for Security-Cleared Professionals Levels off Despite Strong Headwinds.” http://www.clearancejobs.com/files/ClearanceJobs_Compensation_Survey_2014.pdf.
- Libicki, Martin C., David Senty, and Julia Pollak. 2014. *Hackers Wanted: An Examination of the Cybersecurity Labor Market*. Santa Monica, CA: RAND Corporation.
- Linn, Robert A. 2009. “Information Warfare Officer Retention: Using a Capabilities-Based Assessment to Solve Retention Issues.” Master’s thesis, Naval Postgraduate School.
- Obama, Barack. December 11, 2013. “Cybersecurity.” <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity>.
- Paul, Christopher, Isaac R. Porche III, and Elliot Axelband. 2014. *Change by Design. How Design Thinking Transforms Organizations and Inspires Innovation*. Santa Monica, CA: RAND Corporation.
- Pink, Daniel H. 2009. *Drive: The Surprising Truth about what Motivates Us*. New York, NY: Penguin Group (USA).
- Pivot Learning Partners. 2013. “Pivot Learning Partners’ Design Cycle: A Tool for Change” http://pivotlearningpartners.org/sites/default/files/PivotChangeDesign-2013_0.pdf.
- Ramlall, Sunil. 2004. “A Review of Employee Motivation Theories and their Implications for Employee Retention within Organizations.” *The Journal of American Academy of Business* 9: 21–26.
- Riebel, David. 1996. “An Analysis of the Effects of Increases in Aviation Bonuses on the Retention of Naval Aviators Using an Annualized Cost of Leaving (ACOL) Approach.” PhD dissertation, Monterey, CA: Naval Postgraduate School.

- Ritchie, Jane, Jane Lewis, Dawn Snape, Liz Spencer, Robin Legard, Jill Keegan, Kit Ward, Gillian Elam, and William O'Conner. 2003. *Qualitative Research Practice. A Guide for Social Science Students and Researchers*. Thousand Oaks, CA: Sage Publications.
- Samuel, Michael O., and Crispin Chipunza. 2009. "Employee Retention and Turnover: Using Motivational Variables as a Panacea." *African Journal of Business Management* 3(8): 410–415.
- Salem, Anita, M. September 22, 2014. Presentation on Design Thinking Conducted during NPS Workshop.
- Sanborn, James K. 2014. "Tactical Hackers: Cyber Steps up its Role on the Battlefield." *Marine Corps Times*, 18–19.
- Semper Secure. August 5, 2013. "Cyber Security Census." <http://www.sempersecure.org/news/research.html>.
- Skelton, Ike. 1999. "Military Retention Intangibles: Esprit, Morale and Cohesion." *Military Review* 79(4): 2.
- Strauss, Anselm, and Juliet Corbin. 1998. *Basics of Qualitative Research. Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications.
- Suby, Michael. 2013. "The 2013 (ISC)² Global Information Security Workforce Study" (A Frost & Sullivan Market Study). <https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf>.
- Thomas, Kenneth. 2009. "The Four Intrinsic Rewards that Drive Employee Engagement." *Ivey Business Journal Online* 73(6): 1–6.
- Thomas, Kenneth, and Erik Jansen. 1996. "Intrinsic Motivation in the Military: Models and Strategic Importance" (No. NPS-SM-96-001). Monterey, CA: Naval Postgraduate School.
- Turk, Robert. 2013. "Preparing a Cyber Security Workforce for the 21st Century." Master's thesis, United States Army War College.
- United States Marine Corps, Manpower and Reserve Affairs. 2014. *MARADMIN 296/14: MCBUL 7220. Fiscal Year 2015 (FY15) Selective Reenlistment Bonus/(SRB) Program and FY15 Broken Service SRB (BSSRB) Program*. <http://www.marines.mil/News/Messages/MessagesDisplay/tabid/13286/Article/166215/mcbul-7220-fiscal-year-2015-fy15-selective-reenlistment-bonusrb-program-and-fy.aspx>.

- Washington Post. 2003. "Timeline: The U.S. Government and Cybersecurity." <http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html>. Dec 11.
- Waterman, Jr., Robert H., Thomas J. Peters, and Julien R., Phillips. 1980. "Structure is not Organization." *Business Horizons* 23(3): 14–26.
- Westermeyer, Roger H. 2008. "Recruiting and Retaining Cyberwarriors." Master's thesis, United States Army War College.
- White House. December 11, 2013. "Cybersecurity." <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity>.
- Wilshusen, Gregory C. and Valerie C. Melvin. 2011. *Cybersecurity Human Capital. Initiatives Need Better Planning and Coordination* (GAO-12-8). Washington DC: United States Government Accountability Office.
- Zimmerman, B. 2008. "Integrating Monetary and Non-Monetary Reenlistment Incentives Utilizing the Combinatorial Retention Auction Mechanism (CRAM)." Master's thesis. Monterey, CA: Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California